

CONTINUATION OF APPLICATION FOR SEARCH WARRANT

I, Marcel Behnen, being duly sworn, depose and state that:

INTRODUCTION

1. I make this continuation of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—cellular telephones, as described in Attachment A - that are currently in the possession of law enforcement, and the extraction of electronically stored information from that property as described in Attachment B.

2. I am a Task Force Officer with the United States Drug Enforcement Administration, United States Department of Justice, and have been so since March 2019. I have been a police officer with the Kalamazoo Department of Public Safety for about 12 years, the last 3 of which I have been assigned as an investigator with the Kalamazoo Valley Enforcement Team (KVET), which is tasked with investigating narcotics trafficking. I am currently assigned to the Grand Rapids District Office in the DEA's Detroit Field Division. During my time as a KVET Investigator, I have participated in investigations of unlawful drug trafficking and, among other things, have conducted or participated in surveillance, the execution of search warrants, debriefings of informants, reviews of taped conversations and drug records, and have participated in investigations that included the interception of wire and electronic communications. Through my training, education and experience, I have become familiar with the manner in which illegal drugs are transported, stored, and distributed, the methods of payment for such drugs, the

laundering of narcotics proceeds, and the dialect, lingo, and coded language used by narcotics traffickers. In connection with my duties, I investigate criminal violations of the Federal and State controlled substance laws including, but not limited to, conspiracy and attempt to possess with intent to distribute and to distribute controlled substances, in violation of 21 U.S.C. § 846; possession with intent to distribute and distribution of controlled substances, in violation of 21 U.S.C. § 841(a)(1); use of communication facilities to facilitate drug trafficking offenses, in violation of 21 U.S.C. § 843(b), conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h) and money laundering, in violation of 18 U.S.C. § 1956(a)(1)(A)(i), 18 U.S.C. § 1956(a)(1)(B)(i), and 18 U.S.C. § 1957.

3. I respectfully submit that there is probable cause to believe that Jerome ANDERSON has engaged in the distribution of, and in the possession with intent to distribute, crystal methamphetamine, and that he has conspired to do the same, in violation of 21 U.S.C §§ 841(a)(1), 846. I further submit that there is probable cause to believe that evidence of this offense will be found on the cell phones described in Attachment A.

4. The facts in this continuation come from my personal observations, my training and experience, and information obtained from other law enforcement officers, agents, and witnesses. This continuation is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. This continuation supports the application of the warrants to search the property — three cellular telephones — currently in the possession of law enforcement, hereinafter collectively referred to as “the Devices”:

- **Device 1:** Blue/Black Samsung, Model SM-A102U, IMEI 359620103468478 with the phone number (269) 443-9856
- **Device 2:** Blue/Black Motorola XT1952-6, IMEI 357204101270145 with the phone number (269) 569-9423
- **Device 3:** White/black/Chrome Apple iPhone X, unknown model with unknown phone number

6. The Devices are currently located at the Kalamazoo Valley Enforcement Team (KVET, 150 E Crosstown Parkway, Kalamazoo, MI, 49001). The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. On January 24, 2020, investigators with the Kalamazoo Valley Enforcement Team (KVET) arranged the purchase of two ounces of crystal methamphetamine from Jerome ANDERSON utilizing a confidential source (the KVET CS).¹ The KVET CS contacted ANDERSON at phone number 269-569-9423

¹ Investigators believe that the KVET CS is a reliable source of information because the CS has provided KVET with accurate information that has led to the seizure of narcotics, as demonstrated in the controlled purchases from ANDERSON. The

(later determined to be **Device 2**) to place the methamphetamine order. Investigators surveilled the KVET CS to a predetermined location where the KVET CS was observed entering ANDERSON's vehicle. The KVET CS exited ANDERSON's vehicle after approximately one minute, returned to his/her vehicle, and, after constant surveillance, met with KVET investigators to turn over a crystalline substance that field tested positive as methamphetamine. The KVET CS also confirmed it was ANDERSON in the vehicle and whom he/she purchased the methamphetamine from.

8. On March 18, 2020, KVET investigators arranged a second controlled buy of four ounces of crystal methamphetamine from Jerome ANDERSON utilizing a KVET CS. The KVET CS contacted ANDERSON at phone number 269-443-9856 (later determined to be **Device 1**) to place the order. Investigators surveilled the KVET CS to a predetermined location. Eventually, ANDERSON arrived to the location and the KVET CS entered ANDERSON's vehicle and after a short term contacted the KVET CS exited ANDERSON's vehicle, returned to his/her vehicle. After constant surveillance, the KVET CS then met with KVET investigators to turn over a crystalline substance that field tested positive as methamphetamine. KVET investigators confirmed it was ANDERSON driving the vehicle through personal observation and the KVET CS confirmed it was ANDERSON in the vehicle and whom he/she purchased the methamphetamine from.

KVET CS is cooperating with law enforcement in the hope of receiving leniency on pending state criminal charges.

9. On March 19, 2020. KVET investigators executed residential search warrants issued by a Kalamazoo County judge, including a warrant to search 321 E Frank St, Kalamazoo, MI.² Investigators surveilled ANDERSON arrive at 321 E Frank St., enter the residence, and exit a short time later. While walking back to his vehicle, investigators moved in to execute the search warrant. Upon seeing the investigators, ANDERSON began to back pedal, immediately put his hands into his clothing, and turn to run away from the KVET vehicle/investigators. ANDERSON began running back to the west door of 321 E Frank and eventually fell to the ground and was detained/handcuffed. ANDERSON appeared to have dropped three cell phones on the ground, which I collected as evidence (**Device 1**, **Device 2** and **Device 3**).

10. Upon canvassing the area where ANDERSON had first seen investigators, investigators located a baggie of crystal methamphetamine underneath his vehicle (27.94 grams of methamphetamine per the KDPS crime lab).

11. Inside the 1st floor washroom of 321 E Frank St, I located a black backpack in which I located a grocery bag. Inside the grocery bag were three other bags (two knotted sandwich bags, one vacuumed sealed bag) of crystal methamphetamine (551.93 grams total of methamphetamine per the KDPS crime lab).

² Among other facts establishing probable cause, the affidavit in support of this search warrant showed that ANDERSON made frequent trips to 321 E Frank St., and travelled to and from it immediately before and after the March 18, 2020 controlled buy.

12 On this day, ANDERSON was arrested on state charges of possession with intent to deliver methamphetamine. **Devices 1, 2, and 3**, which ANDERSON dropped, were seized by KVET, secured in a KVET cell phone evidence locker, and have remained in law enforcement custody since this date.

13 On April 30, 2020, I received subscriber information through a DOJ administrative subpoena regarding phone numbers contacted by the KVET CS to arrange the controlled buys of methamphetamine from ANDERSON on January 24, 2020 (269-569-9423) and March 18, 2020 (269-443-9856). According to these records provided to me by T-Mobile:

- a. Phone number 269-443-9856 had an assigned device of a “SAM A10E 32G BLK TMUS KIT RSU” with an IMEI of 359620103468478, which matched **Device 1** which ANDERSON dropped prior to his arrest/detainment.
- b. Phone number 269-569-9423 had an assigned device of a “MOT G7 PLY 32GBLU TMUS KIT RSU” with an IMEI of 357204101270145, which matched **Device 2** which ANDERSON dropped prior to his arrest/detainment.
- c. Both phone numbers/devices had a subscriber/account name of “James Jone,” which I believe to be a fictitious name.

14 Based on my training and experience, I know that drug traffickers frequently use more than one cell phone to conduct their drug trafficking business. For example, I have encountered drug dealers that use one cell phone/phone number

to communicate with their suppliers, and a separate cell phone/phone number to communicate with their customers. I have also encountered drug dealers who use one cell phone/phone number for certain customers and co-conspirators with whom they have long-standing relationships that the drug dealers believe are more trustworthy, and a separate cell phone/phone number to communicate with lesser known and lesser trusted customers.

15. Further, based upon my training, experience, and participation in drug investigations and financial investigations relating to drug investigations, I am aware of the following:

- a. Drug traffickers often keep names, aliases, and/or contact information of suppliers, purchasers, and others involved in drug trafficking in their devices;
- b. Drug traffickers sometimes use electronic messaging or messaging apps, in addition to MMS, SMS text messages, and voice call, to communicate with suppliers, purchasers, and others involved in drug trafficking on their devices;
- b. Drug traffickers often take pictures or videos of their drug trafficking associates, drugs, money and/or firearms, which they store on their devices;
- c. That drug traffickers often maintain, on hand, large amounts of currency in order to maintain and finance their on-going narcotics business;

- d. Global Position System (GPS) data on phones may show the location of a drug trafficker at a given time, which may provide corroborating evidence of a drug delivery or other instance of drug trafficking;
- e. User attribution data and usernames, passwords, documents, and browsing history can provide evidence that the device is being used by a drug trafficker and can provide other useful evidence to the drug investigation;
- f. Drug traffickers often use the internet to look up various information to support their drug trafficking activities;
- g. That drug traffickers often have unexplained wealth and assets as they do not have a job, nor do they report income on their state or federal tax returns. Subjects often use cash, money orders, and cashier's checks, and prepaid debit cards as a way of purchasing items as a way to disguise where the funds are ultimately coming from. Subjects will place assets in the names of nominees, which are often friends and family members in an attempt to hide the true ownership of the assets. It is common for drug traffickers to maintain books, records, receipts, notes, ledgers, receipts relating to the purchase of financial instruments and or the transfer of funds, and other papers relating to the transportation, ordering, sale and distribution of controlled substances. That the

aforementioned books, records, receipts, notes, ledgers, etc., are maintained where the traffickers have ready access to them, including their devices;

- h. That it is common for persons involved in drug trafficking to maintain evidence pertaining to their obtaining, secreting, transfer, concealment and or expenditure of drug proceeds. This evidence includes currency, financial instruments, precious metals and gemstones, jewelry, books, records, invoices, receipts, records of real estate transactions, bank statements and related records, passbooks, money drafts, letters of credit, money orders, bank drafts, cashier's checks, bank checks, safe deposit box receipts or keys, records concerning storage lockers and money wrappers. These and other items are maintained by the drug traffickers within their residences, businesses, or other locations over which they maintain dominion and control.
- i. That when drug traffickers amass large proceeds from the sale of controlled substances that the drug traffickers attempt to legitimize these profits through money laundering activities. To accomplish these goals, drug traffickers utilize but are not limited to, domestic and international banks and their attendant services, professionals such as attorneys and accountants, casinos, real estate, shell corporations and business fronts,

storage lockers, safe deposit boxes and otherwise legitimate businesses that generate large quantities of currency.

- j. That the sale of controlled substances generates large quantities of United States currency in small denominations (commonly referred to as “street money”).
- k. That it is common for drug traffickers to separate their “street money” by denomination and organize this currency in rubber banded stacks in varying \$1,000 increments to facilitate quick counting.
- l. That the courts have recognized that the small and medium denominations of questionable currency, along with the manner in which the currency is handled, carried and concealed may establish probable cause that there is a substantial connection between the questionable currency and drug transactions.
- m. That drug traffickers at times become fearful that their extravagant spending habits will bring them under scrutiny by the Internal Revenue Service or other federal, state, or local agencies. The “source” of their income reported on tax returns can be falsely stated, misleading or generic in terms. Retained copies of these returns are commonly kept by the traffickers in their residences and businesses.

- n. That the courts have recognized that unexplained wealth is probative evidence of crimes motivated by greed, in particular, trafficking in controlled substances.
- o. That drug traffickers frequently receive their supply of drugs through packages sent by U.S. Mail or third-party delivery service.

TECHNICAL TERMS

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing

back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can

also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses,

appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while

other computers have dynamic—that is, frequently changed—IP addresses.

- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

17. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online, I know that the Devices have capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and/or PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also

forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information

necessary to understand other evidence also falls within the scope of the warrant.

- Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

21. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

22. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.